IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s):	Messaoud Benantar		
Assignee:	International Business Machines Corporation		
Title:	Method and System for Computing Digital Certificate Trust Paths Using Transitive Closures		
Serial No.:	10/045,112	Filing Date:	January 10, 2002
Examiner:	Shin Hon Chen	Group Art Unit:	2131
Docket No.:	AUS920010943US1	Customer No.	65362

FILED ELECTRONICALLY

Austin, Texas
August 27, 2008

PRE-APPEAL BRIEF REQUEST FOR REVIEW AND STATEMENT OF REASONS

Sir:

Applicants request review of the Final Office Action dated May 27, 2008, in the above-identified application. No amendments are being filed with the request. This request is being filed with a Notice of Appeal. The following sets forth a succinct, concise, and focused set of arguments for which the review is being requested.

CLAIM STATUS

In the Final Office Action, claims 1-36 were rejected as anticipated by U.S. Patent No. 6,134,550 to Van Oorschot et al. ("Oorschot"). Applicant respectfully traverses the rejection for the reasons set forth hereinbelow.

A. The "Transitive Closure Computation" Requirement Variously Recited In Claims 1-9, 24, 27, and 30 Is Not Anticipated by Oorschot

In response to the anticipation rejection of claims 1-9, Applicant respectfully submits that Oorschot's disclosed system (for employing trusted paths to determine the validity of a certificate) does not anticipate the present invention's scheme for computing digital certificate trust paths by "performing a transitive closure computation on the adjacency matrix to generate a set of inter-CA trust path indicators that represent whether a trust path exists between a pair of certificate authorities." In rejecting claims 1-9, 24, 27, and 30, the Examiner asserted that both the "transitive closure computation" and the "all-pairs-shortest-paths" computations were met by the same passage from Oorschot, namely col. 4, lines 52-57. *See*, Final Office Action, p. 2. In

response to Applicant's explanation that the "transitive closure computation" requirement is *separate* from the all-pairs-shortest-paths computation, the Examiner now asserts that Oorschot's disclosure of a "compilation of certificate chain data to generate a table of trusted relationships among the certificate issuing units (VO: column 4 lines 52-62)" meets the claimed "transitive closure computation" requirement, and that "the compilation of certificate chain data is different from the shortest-path computation (VO: column 4 lines 65-67) in which the compilation of certificate chain data takes place before the shortest-path computation to ensure validity of path." *See,* Advisory Action, p. 3. With all due respect, the shift in the Examiner's latest rejection analysis to cite different passages from Oorschot appears to be improperly driven in hindsight by Applicant's explanation, not by any legitimate reading of Oorschot's disclosure. Indeed, when the *entirety* of the cited Oorschot passage is considered, it becomes apparent that the "shortest trusted path" is an example of what is generated when Oorschot's certificate chain data is compiled:

> For example, where a high degree of compilation is performed, the certificate chain data may be a list of all certification authorities in a shortest trusted path starting with a subscriber's own CA and ending with the target CA that issued the certificate of the subscriber that sent a digitally signed message. The compiled certification authority trust data serves as certificate chain data that may be for example, a table of trust relationships among the certificate issuing units in a community of interest, to facilitate rapid validity determination of the certificate by a plurality of requesting units. By way of example, the compilation may consist of populating a database that can be repeatedly queried by multiple subscribers to provide a preferred chain of certificates in a shortest trusted path among two subscribers, or between their respective CAs. If preferred, the stored certificate chain data can also include the associated certificates, or other information such as revocation status information related to the associated certificates, for each of the certificate issuing units listed in the table.

Oorschot, col. 4, lines 52-67 (emphasis added). As the passage shows, the referenced compilation of certificate chain data from Oorschot is not separate from the "all-pairs-shortest-paths" computation, and therefore does not anticipate the separately claimed requirement of "performing a transitive closure computation." As claimed and described by Applicant, the recited "transitive closure computation" is distinct from the "all-pairs-short-path" computation, and is used to determine, before the actual path is determined, whether there is a path through the directed graph for any two certificate authorities in the directed graph. *See*, Application, paragraphs 70-76. Applicant submits further that those skilled in the art would understand that the transitive closure algorithm differs from the shortest path algorithm in that Oorschot requires

storing the pairs of shortest paths, while the transitive closure calculations are simpler since they only deal with a true or false answer (where true means there is a path between two nodes and false otherwise) so that the transitive closure only needs to store the boolean true or false for each given pair of CA certificates (0, or 1) that can be minimized to the bit-wise level.

Accordingly, Applicant respectfully submits that this omission amounts to a failure to articulate a *prima facie* anticipation showing that each and every element of the claimed invention, arranged as required by claims 1-9, 24, 27, and 30, are found in the Oorschot reference, either expressly or under the principles of inherency. *See generally*, In re King, 801 F.2d 1324, 1326, 231 USPQ 136, 138 (Fed. Cir. 1986); Lindemann Maschinenfabrik GMBH v. American Hoist and Derrick, 730 F.2d 1452, 1458, 221 USPQ 481, 485 (Fed. Cir. 1984). Because of at least these differences between Oorschot and claims 1-9, 24, 27, and 30, Applicant requests reconsideration and withdrawal of the anticipation rejection of claims 1-9, 24, 27, and 30.

B. The Requirement That A Certificate Authority Send "A Trust Relation Update Message To A Central Trust Web Agent" Variously Recited In Claims 10-30 Is Not Anticipated by Oorschot

In response to the anticipation rejection of claims 10-30, Applicant respectfully submits that Oorschot's disclosed system (for employing trusted paths to determine the validity of a certificate) does not anticipate the present invention's scheme for computing digital certificate trust paths by, *inter alia*, having a certificate authority send "a trust relation update message to a central trust web agent, wherein the central trust web agent processes trust relation information for a set of certificate authorities within a trust web," as variously recited in claims 10-30. Nor does Oorschot disclose "modifying a set of trust relations for the set of certificate authorities within the trust web based on an indicated request in the trust relation update message," as variously recited in claims 22-30. In rejecting claims 10-30, the Examiner cites Oorschot's disclosure (col. 5, lines 53-61, col. 6, lines 1-11, and col. 7, line 62 to col. 8, line 13) that the certificate chain data 209 and database 208 can be "periodically updated." *See*, Final Office Action, pp. 3-4. In response to Applicant's explanation that the claim requirements for the "trust relation update message" are not met by Oorschot, the Examiner now asserts that Oorschot (col. 5, lines 53-61, col. 6, lines 1-11) discloses that "the CAs respectively provide certificate chain information to the central web agent for compilation and periodically provide update to the central agent in order to establish the up-to-date certificate chain data." *See,* Advisory Action, p.

3. However, as seen from the cited Oorschot passage which is set forth below, there is simply no reference in Oorschot of having a certificate authority send a "trust relation update message" to a central trust web agent, much less using the received "trust relation update message" to modify the set of trust relations at the central trust web agent:

> The certificate chain data 209 is compiled from certification authority trust data. Certification authority trust data may include for example, cross-certification data, revocation data and/or other data stored in a distributed directory (e.g., X.500 directories or LDAP-compliant repositories). The certificate chain data 209 is prepared once, and periodically updated as needed, for more than one subscriber and may be repeatedly used each time validation needs to occur.
>
> * * *
>
> .... The certificate validating unit 204 sends a query in the form of a request signal to the certificate chain constructing unit 206 to obtain certificate chain information relating to a preferred certificate chain between certificate issuing units in a trusted path in a community of interest. The certificate chain constructing unit 206 analyzes the certificate chain data 209 stored in the certificate chain data storage medium 208 and transmits certificate chain information to the certificate validation unit 204 to allow the certificate validation unit to determine the validity of the certificate to be validated in a rapid fashion.
>
> The certificate chain database 208 may be periodically updated, for example by the certificate chain data generator 400 periodically polling the distributed directory 302 or other sources of certificate data to determine whether updates in the certificate trust data has occurred (additional certificates, revocation of certificates etc.) and recompiling the necessary database entries. For example, if a certification authority (CA) is added to the community of interest, the certificate chain data generator 400 obtains the new information from the directory 302 and adds any links based on the certification authority trust data associated with that new certificate issuing unit to incorporate the trust relationship as certificate chain data 209 in the certificate chain data database 208. Therefore where a database 302 includes certificates indicating cross-certification among certificate issuing units, the certificate chain data generator 400 uses the cross-certification information to note a trust path between the corresponding certificate issuing units.

Oorschot, col. 5, lines 53-61, col. 6, lines 1-11, and col. 7, line 62 to col. 8, line 13 (emphasis added). Indeed, Oorschot discloses a variety of techniques for updating the certificate chain database 208 (including periodically polling the distributed directory or other sources of certificate data), but conspicuously fails to disclose using trust relation update messages from the certificate authorities. In contrast, Applicant has distinctly claimed and described the role of the "trust relation update message" in "modifying a set of trust relations for the certificate authorities." *See*, Application, paragraphs 95-97.

While Applicant has distinctly recited the requirement of a "trust relation update message" that is sent to or received by a central trust web agent which "processes trust relation information for a set of certificate authorities within a trust web" in claims 10-30, the Final Office Action omits any explanation of how Oorschot anticipates this claim requirement. Nor does the Final Office Action explain how Oorschot discloses the requirement of "modifying a set of trust relations for the set of certificate authorities within the trust web based on an indicated request in the trust relation update message" recited in claims 24-30. Accordingly, Applicant respectfully submits that this omission amounts to a failure to articulate a *prima facie* anticipation showing that each and every element of the claimed invention, arranged as required by claims 10-30, are found in the Oorschot reference, either expressly or under the principles of inherency. *See generally*, In re King, 801 F.2d 1324, 1326, 231 USPQ 136, 138 (Fed. Cir. 1986); Lindemann Maschinenfabrik GMBH v. American Hoist and Derrick, 730 F.2d 1452, 1458, 221 USPQ 481, 485 (Fed. Cir. 1984). Because of at least these differences between Oorschot and the claims, Applicant requests reconsideration and withdrawal of the anticipation rejection of claims 10-30.

CONCLUSION

In view of the remarks set forth herein, Applicant respectfully submits that all pending claims are in condition for allowance and request that a Notice of Allowance be issued. Nonetheless, should any issues remain that might be subject to resolution through a telephonic interview, the examiner is requested to telephone the undersigned at 512-338-9100.

CERTIFICATE OF TRANSMISSION

I hereby certify that on August 27, 2008 this correspondence is being transmitted via the U.S. Patent & Trademark Office's electronic filing system.

/Michael Rocco Cannatti/

Respectfully submitted,

/Michael Rocco Cannatti/

Michael Rocco Cannatti
Attorney for Applicant(s)
Reg. No. 34,791